PARADOJAS (Tribuna de Astronomía y UNIVERSO 35 - mayo 2002)

CRIPTOGRAFÍA NOVELADA

Miquel Barceló

Los seres humanos siempre han querido proteger de miradas ajenas el contenido de algunos de los mensajes que se transmitían entre sí. Pero muy pronto resultó evidente el peligro y la insuficiencia que representaba dejar la responsabilidad de mantener tal secreto en manos del mensajero, por fiable que éste pudiera parecer o resultar. El secreto de los mensajes debía residir en el mensaje mismo, y de ahí los diversos sistemas de cifrado que, a lo largo de los siglos, han intentado lograr que el contenido real del mensaje transmitido sólo fuera conocido por su verdadero destinatario.

Famoso es el elemental sistema de cifrado que utilizara Julio César hace ya más de 2000 años en algunas de sus comunicaciones a Cicerón y a determinados cónsules. El sistema consistía, simplemente, en sustituir cada letra por la tercera que le sigue (de forma cíclica) en el alfabeto. Así JUEZ se cifraría como MXHC. Se trata de un sistema sencillo y claramente vulnerable que hace francamente fácil la labor del descifrado.

Fueron precisamente las dos guerras mundiales del siglo XX las que proporcionaron un impulso decisivo a la criptografía y, en especial, a las técnicas criptoanalíticas de descifrado de mensajes. En 1919, el mecánico berlinés Arthur Scherbius construyó la primera versión de ENIGMA, una máquina criptográfica que acabó siendo usada por la marina alemana durante la Segunda Guerra Mundial para, por ejemplo, dar órdenes a los submarinos del Atlántico respecto de los convoyes a atacar. Posiblemente el primer gran reto al que se enfrentó la criptografía moderna.

El ENIGMA parecía una máquina de escribir convencional, pero un conjunto interno de rotores convertía la letra tecleada en la que le correspondía según una determinada codificación. El receptor del mensaje cifrado, si disponía de la misma clave (relacionada con la disposición inicial de esos rotores), obtenía el texto original con su máquina ENIGMA convenientemente configurada.

El matemático británico Alan Mathison Turing fue uno de los primeros grandes especialistas en las labores de descifrado para las cuales, desde 1939, se creó en Bletchley Park un centro que llegó a ocupar casi 6000 personas en el duro trabajo de descifrar los radiogramas alemanes cifrados con el ENIGMA.

Pero ése es sólo el principio de la criptografía moderna y su compleja base matemática, un saber hoy del todo imprescindible para la seguridad de la nueva sociedad de la información con el uso fiable de la red Internet.

Junto a los problemas básicos de las técnicas criptográficas, hay que considerar también la curiosa mentalidad de quienes responden con dedicación casi monomaníaca al reto de descifrar mensajes creados precisamente para no ser descifrados. Una personalidad sorprendente y un complejo sistema de motivaciones psicológicas parece concurrir en quienes se dedican a esa compleja y difícil labor.

Llevar todo ese mundo de matemática, lógica y desafío intelectual al ámbito narrativo es también un descomunal reto que parece haber afrontado con éxito el estadounidense Neal Stephenson con su "*Criptonomicón*", la novela seleccionada como la mejor del año 2000 por los lectores de la influyente revista LOCUS. Se trata de una novela sin igual, que ahora ve la luz en castellano y que ha sido considerada algo así como el nuevo libro de culto de los hackers, y su autor como "*el Hemingway de los hackers*" y el "*Quentin Tarantino de la ciencia-ficción post-ciberpunk*".

Stephenson, conocedor como pocos del mundillo de los hackers y de las complejidades de una futura sociedad informatizada, recurre a una amena prosa cargada del humor más irónico, para ofrecernos al mismo tiempo una divulgación criptográfica brillante y, también, el difícil y ajustado

retrato de la mentalidad y los preocupaciones de matemáticos, informáticos, militares y empresarios de alta tecnología involucrados en los sistemas criptográficos. Tal como se ha dicho en la red, Stephenson convierte la ética hacker en una novela épica a la que ya se han buscado incluso semejanzas estructurales y de personajes con la hoy cinematográfica "*El señor de los Anillos*" de Tolkien.

En "*Criptonomicón*", Stephenson imagina que, en 1942, Lawrence Pritchard Waterhouse, un genio matemático y capitán de la Marina estadounidense, colabora con Alan Mathison Turing y los especialistas británicos de Betchely Park en el trabajo de descifrar los códigos secretos de las potencias del eje. Paralelamente, aunque sesenta años más tarde, la empresa de su nieto y también brillante cripto-hacker, Randy Waterhouse, proyecta crear, en una isla del sudeste asiático, la Cripta, un nuevo paraíso de datos y el mayor exponente de la libertad informática del futuro.

Si la criptografía puede ser de interés para muchos, lo cierto es que Stephenson la divulga brillantemente al tiempo que disecciona con suma habilidad la mentalidad de algunos personajes tocados por la gracia de la matemática y de la habilidad criptográfica.

Tal y como se solía decir de una famosa revista, se trata de "*la novela más audaz para el lector más inteligente*". Se la recomiendo encarecidamente.